GEOCOMPLY

September 12, 2017

Michigan State Rep. Brandt Iden
House Committee on Regulatory Reform

Dear Chairman Iden and Members of the House Committee on Regulatory Reform,

RE: Testimony on the Role of Geolocation Technology for Internet Gaming in Michigan

As Michigan considers the introduction of internet Gaming, GeoComply submits the testimony material below detailing the role and effectiveness that geolocation technologies play in establishing and regulating a state internet gaming regime. GeoComply is routinely called upon as an expert witness by state and federal legislatures to demonstrate solutions to common issues (and misunderstandings) about geolocation technologies; and to speak to the ability to maintain compliance with federal and state regulations with the correct implementation of appropriate regulations.

Why is Geolocation Important for Michigan?

In this regard, our technology can be used to both **enable** and **restrict** iGaming, and is actively upholding current Michigan state laws as we speak. Our live system deployed by 100% of the regulated US iGaming market is currently blocking access to all individuals physically located within Michigan's borders, per existing state and federal regulations.

GeoComply's advanced and adaptive geolocation solutions are designed as tools for iGaming stakeholders to meet and exceed industry standards when it comes to securely geo-fencing geographic borders. Our technology is uniquely tailored to match complex legal and regulatory requirements; providing government officials, as well as gaming operators, with assurance that their online gaming enterprises are fully compliant with the applicable laws and regulations by providing a more precise, reliable solution than any other geolocation provider serving the gaming space. In-built tools are available to apply specialized filters to users from tribal lands or other specially designated geographic zones.
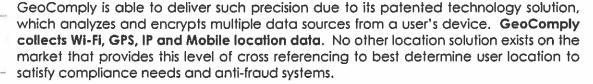
Executive Summary

Since launching in 2011, GeoComply has quickly become the iGaming industry's trusted solution for location compliance, accuracy, and reliability. Its proprietary and highly adaptive technology has successfully met and exceeded all challenges put forth by US regulators with record-high pass rates exceeding 98%. GeoComply currently holds licenses as a geolocation provider from regulators in the states of New Jersey, Nevada, and Delaware, as well as the Georgia Lottery.

How Does Geolocation Work?

Wi-Fi

GeoComply is able to deliver such precision due to its patented technology solution, which analyzes and encrypts multiple data sources from a user's device. **GeoComply collects Wi-Fi, GPS, IP and Mobile location data**. No other location solution exists on the market that provides this level of cross referencing to best determine user location to satisfy compliance needs and anti-fraud systems.

GPS

MOBILE

Due to the inherent difficulty of accurate geolocation on the internet for regulated industries, sole reliance upon one data source presents an increased risk of inaccurate or imprecise results. We therefore confirm the integrity of location data to ensure it is secure and has not been masked or tampered with by any host of "spoofing" tools such as **proxies, VPNs, remote desktop software, jailbroken devices, fake location apps, mock location settings, developer tools, anonymizers**, on so on. By the time a transaction is approved or denied, the data may have gone through over 350 checks that our compliance algorithm seeks to verify.

IP

"GeoComply were able to cut our payment fraud costs by at least 85%. Their solution gave us access to more detail and data than we had ever had before for our eCommerce transactions. Their anti-fraud reports were literally good enough to take to the bank in order to win our charge back disputes!"
- Omer Sattar, Senior VP, Sightline Payments

Location Code of Conduct

Below is a recommended framework for implementing geolocation regulations with respect to federal and state compliance requirements and considerations; and recognizes the modern-day vulnerabilities of locating online users;

- Geolocation solutions used must always be accurate enough to locate player as **definitely within the permitted State's Borders**
  - **"Bleeding" across borders** will not be tolerated so the highest accuracy methods of geolocation are preferred (WiFi and/or GPS, rather than Cell Tower triangulation and/or GSM).
  - if data Accuracy Radius returned is not accurate enough and/or it overlaps with a bordering State the end user will be blocked.
  - Boundary definitions (geographic coordinates) should be obtained from a state or Federal Government database.

- Any solution used can not be **"self-certified"** but must be independently verified, via Field Tests, as meeting standards required by UIGEA/DOJ requirement for sufficient geolocation tools;
  - Independent verification should be from a body such as a state approved testing facility or government testing facility.
  - Independent Verification must include field trials with common location spoofing methods (inc. those listed in this document).

- IP Geolocation is not acceptable as the sole location data source (as it has the highest risk of vulnerability) without significant additional checks
  - IP location data cannot be considered for mobile (3G) transactions as it represents the location of the carrier and not the end user device.

1530-666 Burrard St   GeoComply.com
Vancouver, B.C.   solutions@GeoComply.com
V6C 2X8   +1 604.336.0877

- o   Additional verification must be more than just a database of known Proxies (as these are so incomplete). Multiple measures such as DNS Proxy Detection, Proxy Piercing, Algorithmic Analysis for Probability of Fraud etc would ALL have to be used to accept IP from Static ISP's as a usable form of Geolocation data.

- Use of an end user's "billing address", residence, or KYC history in an allowed territory is not an acceptable method of geolocation.

- For native applications. the geolocation solution used must be able to analyze the programs running on the device to detect location spoofing applications, and recognize whether the device has been compromised, e.g. a rooted or jail-broken smart phone.
  - o   "VPN Protection" shall be used; VPNs and other methods of location spoofing such as Proxies, DNS Proxies, Remote Desktop Programs, etc must be detected and blocked.

- Mobile/3G connected players (including players on a Laptop with a mobile hotspot or USB dongle on a train for example) must be recognized as being on a mobile connection (not a Static Landline connection). Their re-location frequency must be established in proportion to their proximity to the nearest border & the earliest time their session could breach the border.

- Data analytics must be carried out to recognize players attempting to spoof location.

- Best practice security measures should be in place to ensure "man in the middle attacks" to emulate a successful geolocation result.
  - o   Including encryption standards, license authentication and effective data analytics

Thank you for your time and consideration on this topic. Please feel free to contact me directly for further information on geolocation technology, as internet gaming regulation continues to be considered for Michigan.

Sincerely,

Lindsay Slader
Operations Manager, GeoComply
lindsay@geocomply.com
+1 604.802.8710